# EXHIBIT B

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF GEORGIA**
**ATLANTA DIVISION**

DONNA CURLING, *et al*.

*Plaintiffs*,

v.

BRAD RAFFENSPERGER, *et al.*,

*Defendants*.

CIVIL ACTION

FILE NO. 1:17-cv-2989-AT

**DECLARATION OF THERESA PAYTON**

Pursuant to 28 U.S.C. § 1746, I, Theresa Payton, make the following declaration:

1.

My name is Theresa Payton. I am over the age of 21 years, and I am under no legal disability which would prevent me from giving this declaration. I have been retained as an expert for the State Defendants in this matter and if called to testify, I would testify under oath to these facts.

2.

I am the Chief Executive Officer of Fortalice Solutions. Fortalice Solutions is a full-service cybersecurity company that offers businesses and governments a

full suite of cybersecurity services, including cybersecurity assessments, vendor assessments, red teaming and penetration testing, review of cybersecurity policies and procedures, and cyber incident response and analysis.

3.

Prior to founding Fortalice, I was Chief Information Officer for The Office of Administration, Executive Office of the President at the White House from 2006-2008, overseeing all information technology and information security functions. I am the co-author of numerous books and articles regarding cyber-security, including Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family, and Protecting Your Internet Identity: Are You Naked Online? I was named one of the 25 Most Influential People in Security by Security Magazine.

4.

State Defendants have articulated a need for their experts to inspect Dr. Halderman's alleged "vote-stealing" malware to prepare a defense in this case. The malware was part of a demonstration during Dr. Halderman's testimony at a September 2018 hearing when he testified about the security of Georgia's elections.

5.

I have reviewed the Court's July 9, 2019 Order regarding the GEMS database and protocols ordered to protect that information, [Doc. 463], and believe Fortalice Solutions can provide identical or even more secure protection of the memory card and alleged malware contained therein.

6.

Fortalice Solutions has a staff of 40 people, including 15 people with experience handling, examining, and evaluating high-risk cybersecurity software and hardware for both governments and private businesses. The types of information we protect includes sensitive and confidential information for the U.S. government and military, state and local government, Fortune 500 companies across a variety of industry verticals, and individuals. Our staff includes individuals with expertise or experience in offensive cyber operations, ethical hacking, network defense, supply chain security, incident response, cyber risk assessment, and open source intelligence analysis including dark web and deep web analysis. Our staff have been senior cybersecurity employees and consultants within large corporate and high-level U.S. government and military environments. Finally, in 2018, Fortalice Solutions made its debut on Cybersecurity Ventures 500 list of top companies at number 250.

7.

In response to the Court's July 16, 2019 Order regarding the security protocols that will be used to protect the memory card, Fortalice Solutions is prepared to implement the following security protocols.

8.

Fortalice will establish a locked, secure work area to which only State Defendants' attorneys and designated experts, or staff assisting in the review under their control and supervision, have access. The entry to the work area will be subject to 24-hour video surveillance and the memory card would be maintained in a locked safe when not in use. A log of all access to the secure work area would be maintained.

9.

The secure work area will include one computer, one PCMCIA duplication unit, and one Direct Recording Electronic voting machine. Each of these items will be clearly marked as Protected, will not leave the secure work area, and will not be used for any election or attached to any election systems after being placed in the secure work area. The computer, duplication unit, and DRE will be air-gapped, password-protected (if available on the particular unit), and not connected to any external or internal network (including wireless access).

10.

State Defendants' attorneys and designated experts, and staff under the direction and control of designated experts, would be permitted to bring their own laptops into the secure work area. Beyond material required to analyze the memory card, no additional equipment or materials would be permitted in the secure work areas.

11.

If Plaintiffs provide only one memory card for the Fortalice Solutions location, State Defendants' designated experts, or staff under the direction and control of the designated experts, will create one duplicate memory card using the PCMCIA duplicator, but will not be permitted to create any other copies of the memory card. If Plaintiffs provide two identical memory cards for the location at Fortalice Solutions, State Defendants will not include a duplicator in the secure work area and will not make any additional copies of the memory card or the software on it.

12.

Under no circumstances would the malware or the information on the memory card be installed on any non-Protected computer, DRE, or other unit. While attorneys and designated experts would be permitted to use external hard

disks and removable storage media (e.g., USB drives, CD-Rs, and DVD-Rs) on their own laptops and other devices, those devices would not be permitted to be installed or connected in any way to a Protected unit.

13.

I and designated staff under my control will conduct any review of the memory card and its contents at the proposed Fortalice location. All designated experts, and staff under the direction and control of designated experts, entering the secure work area would be required to sign confidentiality agreements and be bound by the terms of the Protective Order entered in this case.

14.

In addition to the above-outlined protocols, Fortalice Solutions is prepared to implement any additional restrictions the Court may require.

15.

Mr. Paul Brandau will assist me in this proposed review as Technical Oversight Director. Mr. Brandau is the Advanced Techniques and Training Director at Fortalice Solutions. Mr. Brandau leads two Fortalice security teams in developing and implementing penetration tests and strategies for clients of Fortalice Solutions. Mr. Brandau's past experience includes time as a network malware analyst, incident responder, and penetration tester for other private sector

firms, where he oversaw remediation actions for a high-profile cyber-intrusion into a major foreign government. Mr. Brandau also served as a Captain in the United States Air Force where he developed instruction curricula for offensive and defensive cyber tactics. Mr. Brandau holds a Bachelor of Science degree in Computer Science from Embry-Riddle Aeronautical University and a Master of Science degree from the University of San Diego.

16.

These protocols should be more than sufficient to ensure the security of the memory card and the malware contained on it. In addition, Fortalice Solutions has the experience and capability to ensure these protocols are effectively implemented and enforced.

I declare under penalty of perjury that the foregoing is true and correct. Executed this 16th day of July, 2019.

THERESA PAYTON